BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 10-1101

30 JUNE 2001

AIR FORCE MATERIEL COMMAND
Supplement 1

1 November 2002

Operations

OPERATIONS SECURITY (OPSEC)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication, unsupplemented, is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ USAF/XOIWI (Capt Eric Lambert)
HQ AFMC/SFXP (Marlene K. Meyer)

Certified by: SAF/AAI
(Lt Gen Robert H. Foglesong)
HQ AFMC/SF (Col Leroy L. Walters)

Supersedes AFI 10-1101, 1 May 1997
AFI 10-1101_AFMCS1, 25 Feb 98

Pages: 34
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 10-11, *Operations Security*; DoD Directive 5205.2, *DoD Operations Security Program*, November 29, 1999; Chairman, Joint Chiefs of Staff Instruction (CJCSI) 3210.01A, *Joint Information Warfare Policy*, January 2, 1996;CJCSI 3213.01, *Joint Operations Security*, May 28, 1993; and Operations Security requirements for DoD Instruction 5000.2, *Defense Acquisition Management Policies and Procedures*, October 23, 2000. The reporting requirements in paragraphs **3.6.**, **3.6.1.** and **3.6.2.** are exempt from licensing in accordance with paragraph 2.11.1 of AFI 33-324, The Controlling Internal, Public, and Interagency Air Force Information Collections. The instruction supports AFPD 10-20, *Air Force Defensive Counterinformation Operations*, and related instructions include AFI 33-129, *Transmission of Information via the Internet*, and AFI 33-219, *Telecommunications Monitoring and Assessment Program*. It provides guidance for all Air Force personnel and supporting contractors in implementing and maintaining OPSEC programs. It describes the OPSEC process, and discusses integration of OPSEC into Air Force plans, operations, and support activities. Maintain and dispose of records created as a result of prescribed processes in accordance with AFMAN 37-139, *Records Disposition Schedule.*

(AFMC) This instruction supplements AFI 10-110, *Operations Security*. It explains program management and unique OPSEC requirements in Air Force Materiel Command. This instruction requires the collection and maintenance of information protected by the Privacy Act of 1974. The authority to collect and maintain the data prescribed in this instruction is 10 U.S.C. 8013. This supplement does not apply to the Air National Guard or US Air Force Reserve unit or members.

SUMMARY OF REVISIONS

1. Integrates Operations Security (OPSEC) into Defensive Information Operations (IO).
2. Calls for OMDVA & TMAP to be integrated as part of the IO Red Team concept.
3. Requires annual OPSEC reports to HHQ, annual OPSEC threat product, annual MDCI assessments by HQ's FOSI, annual in-house surveys.
4. Requires each MAJCOM to have written OPSEC plan and provides format.
5. Introduces concept of OPSEC advisories and events and adds requirement for OPSEC reporting IAW AFPD 10-20.
6. Discusses OPSEC & the INTERNET. Requires OPSEC PM to be included in the coordination process for posting data to the NIPRnet/internet and review organizational web pages on annual basis.
7. Clarifies the concept of OPSEC Measures.
8. Discusses role of OPSEC in Force Protection and Antiterrorism.

(AFMC) This supplement is substantially revised and must be completely reviewed. It aligns its guidance with the revised Air Force Instruction 10-1101, 31 May 2001. Revision changes verbiage in DD Form 254, **DoD Contract Classification Specification**, reference to OPSEC requirements in contracts, adds requirement for contracting activities to provide critical information lists to contractors, adds requirement for vulnerability assessments in areas visited by foreign nationals, adds website for Interagency OPSEC Support Staff (IOSS) products, adds date for submission of annual OPSEC report, adds timeframe for HQ AFMC/SFSP OPSEC staff assistance visits (SAVs), and adds the requirement for AFMC units tenant on other MAJCOM installations to participate in the host activity's OPSEC program. A revision is shown by a bar (|).

AFI 10-1101, 31 May 2001, is supplemented as follows:

Chapter 1

INTRODUCTION

1.1. General.. Defensive Counterinformation operations (DCI) are those actions protecting Air Force information and information systems from exploitation by adversaries. The Air Force employs DCI to ensure its ability to conduct operations that are increasingly information dependent. DCI interweaves many related capabilities to meet this objective. OPSEC is one of these capabilities together with information assurance, counterdeception, counterintelligence, counterpsychological operations, and electronic protection.

1.2. Definition.. OPSEC is the process of identifying critical friendly information and analyzing friendly actions related to operations, acquisition, and other activities to identify those actions that can be observed by potential adversaries and determine indicators that could be collected and synthesized to derive critical information in time to be useful to an adversary and eliminate or reduce to an acceptable level the vulnerabilities of friendly information to adversary exploitation.

1.2.1. OPSEC is not a collection of specific rules and instructions. Rather, it is a methodology applicable to any operational activity.

1.3. Characteristics of OPSEC. The goal of OPSEC is to identify information and observable actions relating to mission capabilities, limitations, and intentions in order to prevent exploitation by potential adversaries. Operational effectiveness is enhanced when commanders and other decision-makers apply OPSEC from the earliest stages of planning. OPSEC methodology provides a step-by-step analysis of operations and behavior from an adversary's point of view, thereby assessing how vulnerabilities might be exploited. Information that adversaries need to achieve their goals constitutes critical information about our operations or programs. By identifying and protecting this critical information, the OPSEC process becomes a positive, proactive means by which adversaries are denied an important advantage.

1.3.1. OPSEC involves a series of analyses to examine the planning, preparation, execution, and post execution phases of any activity across the entire spectrum of military action and in any operational environment. OPSEC analysis provides decision-makers with a means of weighing how much risk they are willing to accept in particular operational circumstances.

1.3.1. (AFMC) OPSEC is a key component of Information Operations/Warfare (IO/IW). Coordination with other elements of IO/IW such as Military Deception, Intelligence, and Information Assurance is critical to gain the maximum synergy with increasingly limited resources and the real threat of technology transfer. In today's free-flowing information-based society there are many channels of information easily accessible by potential adversaries. The active use of the internet and information systems to transmit military defense information is a prime example. Factor increasing internet use, web sites, and telephone usage into the organization's overall OPSEC posture. Awareness and continued training are key to successfully protecting critical information (CI) and guarding against its exploitation.

1.3.2. OPSEC should be closely coordinated with the other security disciplines (Physical Security, AFPD 31-1; Acquisition Security, AFPD 31-7; Information Security, AFPD 31-4; Electronic Mail (E-mail) Management and Use, AFI 33-119; Antiterrorism/Force Protection Program, AFI 31-210; Transmission of Information Via The Internet, AFI 33-129 and Information Protection, AFPD 33-2)

to ensure that all aspects of sensitive activities are protected. Also, Public Affairs Policies and Procedures AFI-35-101 chapter 15 (Security Review) and chapter 18 (New Media) should be reviewed. The primary focus of OPSEC analysis is to deny potential exploitation of open source and observable actions. These sources are generally unclassified and, consequently, more difficult to control.

1.3.3. OPSEC is a critical component of DCI that counters the capabilities under the "gain" and "exploit" aspects of an adversary's Information Operations (IO). OPSEC provides a means of identifying critical friendly information and denying an adversary access to that information. OPSEC enables friendly force information superiority by neutralizing adversary information activities, thereby allowing us the unimpeded ability to collect, control, exploit, and defend information.

1.3.3.1. OPSEC should be employed with other complementary IO activities to obtain maximum effectiveness. Planners and commanders should utilize all capabilities (or disciplines) within information operations, including OPSEC in a coordinated effort to control the perceptions and decision-making of an adversary.

1.4. Air Force Operations Security.. The Air Force implements OPSEC in all functional areas. Commanders are responsible for OPSEC awareness throughout their organizations and for integrating the OPSEC process throughout all mission areas. Air Force commanders and decision-makers will consider OPSEC during mission planning, force execution, and throughout the acquisition process. OPSEC will be incorporated into day-to-day activities to the maximum extent possible to ensure a seamless transition to contingency operations.

1.4.1. OPSEC issues are integrated into all aspects of planning and executing air, space, and information operations. OPSEC assists in the protection of Air Force capabilities and intentions by, degrading an adversary's knowledge and subsequent ability to attack our forces or counter our operations. Embedding OPSEC into campaign planning and force execution maximizes mission effectiveness.

1.4.2. OPSEC supports Air Force research, development, test, and evaluation through the reduction of compromised technology and proprietary information. Acquisition organizations that fail to implement OPSEC are more likely to unintentionally reveal critical information, ultimately increasing operational risk as potentially compromised systems are fielded.

1.4.3. OPSEC is also a key component of force protection and antiterrorism. The OPSEC process is an integral part of force protection, helping protect service members, civilian employees, family members, facilities, and equipment at all locations and in all situations. Antiterrorism relies heavily on OPSEC as a means of denying terrorists targeting information. Since force protection and antiterrorism protect the AF's most precious asset--*people,* it is critical that OPSEC be scrupulously applied throughout the Air Force.

Chapter 2

THE OPSEC PROCESS

2.1. General.. OPSEC is accomplished through the use of a five-step process. The five steps of the process are identification of Critical Information and indicators; threat analysis; vulnerability analysis; risk assessment and application of appropriate measures. Although these steps are normally applied in a sequential manner during deliberate or crisis action planning, dynamic situations may require any one to be revisited at any time.

2.2. Identification of Critical Information and Indicators.. Critical information is information about friendly (U.S., allied, and/or coalition) activities, intentions, capabilities or limitations that an adversary seeks in order to gain a military, political, diplomatic, economic, or technological advantage. Such information, if revealed to an adversary prematurely, may prevent or complicate mission accomplishment, reduce mission effectiveness, or cause loss of lives or damage to friendly resources. Critical information usually involves a few key elements of information concerning friendly activities or intentions that might significantly degrade mission effectiveness if revealed to an adversary. Critical information may also be derived from seemingly unrelated elements of information known as indicators.

2.2.1. Critical information is best identified by individuals responsible for the planning and execution of operations. Based on these inputs, commanders must determine and protect their organization's critical information.

2.2.1. (AFMC) AFMC Product, Logistics, Test Center, site, and subordinate unit OPSEC Program Managers (PMs) will develop and distribute commander approved CI lists within their respective organizations. OPSEC PMs review CI, OPSEC indicators, and associated protective measures annually to ensure relevancy to current mission, activities, and procedures and validate the need for continued protection.

2.2.2. Critical information should be identified at the earliest possible time, preferably during the earliest planning phases of an operation. Subordinate and supporting organizations should be apprised of operational information determined to be critical so that they too can protect this information as well as any associated indicators.

2.2.3. A list of elements of critical information will be revised to reflect changing circumstances. While categories of critical information are fairly stable, specific items of information are usually only critical for a prescribed period of time. The need to control or protect specific items of information generally changes as the operation progresses or the OPSEC threat changes.

2.2.4. The Air Force will identify to contractors requirements to control and protect critical information. Contractors will continue to control and protect critical information until the need for OPSEC measures no longer exist.

2.2.4. (AFMC) AFMC organizations must consider OPSEC when issuing contracts for both classified and unclassified programs. When an OPSEC requirement is included in a classified contract, indicate "yes" in block 11j of the DD Form 254. In Item 14, include a statement referencing OPSEC requirements in the contract and indicate that the CIs will be provided to the contractor under separate cover and updated as required. All new unclassified contracts that require on-base performance will include a provision that contractors must participate in the installation's OPSEC program.

Responsible organizational OPSEC PMs will provide contracting activities with lists of the center or site CI. Direct questions regarding OPSEC requirements for contracts including CI to the center or site OPSEC PM.

2.2.5. In most cases, unclassified information identified as critical is described as "Sensitive but Unclassified." Classified information is protected by handling through secure channels, but in some cases even unclassified information should be treated as critical information from an OPSEC standpoint.

2.3. Threat Assessment.. Current threat information is extremely important in developing appropriate OPSEC measures. A global OPSEC threat study will be produced by NAIC on an annual basis. AFOSI will team with NAIC to provide counterintelligence inputs upon request. The OPSEC threat analysis includes identifying potential adversaries and their associated capabilities, limitations, and intentions to collect, analyze and use critical information and OPSEC indicators against friendly forces. The Air Force wide threat study must be used as the basis for an OPSEC threat analysis that is tailored to the operation, test, activity, geographic region, or facility.

2.3.1. The Air Force Office of Special Investigations (AFOSI) produces counterintelligence studies. AFOSI analyzes multi-disciplinary intelligence to evaluate threats from foreign intelligence services. This helps to protect both Air Force and DOD people and resources. AFOSI detachments produce local counterintelligence and criminal threat assessments on an annual basis. These assessments provide valuable input for OPSEC program decisions. AFOSI detachments may also produce focused counterintelligence studies when requested.

2.3.1. (AFMC) Contact the local Air Force Office of Special Investigations (AFOSI) Detachment and the servicing Intel Office to receive current intelligence collection threat information for individual systems, programs, or facilities.

2.4. Vulnerability Analysis.. An operations security vulnerability exists when friendly actions provide indicators that may used by a potential adversary to support their decision-making. Once vulnerabilities are identified, they can normally be mitigated.

2.5. Risk Assessment.. Risk assessment involves an estimate of an adversary's capability to exploit a weakness, the potential effects such as exploitation will have on operations, and a cost-benefit analysis of possible methods to control the availability of critical information to the adversary.

2.5.1. The centerpiece of OPSEC is risk management. OPSEC program managers, in concert with other planners and with the assistance of intelligence and counterintelligence organizations, will provide risk assessments and recommend actions to senior decision-makers and commanders. Commanders must then decide whether or not to employ recommended OPSEC measures.

2.5.2. The guiding principles of Operational Risk Management (ORM), managing all dimensions of risk to maximize mission effectiveness and sustain readiness, must be applied to OPSEC. Applying these principles will ensure that unnecessary OPSEC risks are not accepted and conversely, that OPSEC risks are accepted when costs of mitigating such risks clearly outweigh the benefits.

2.6. OPSEC Measures.. Recommended OPSEC measures are designed to preserve military capabilities by preventing adversarial exploitation of critical information. OPSEC measures are employed to counter vulnerabilities that point to or divulge critical information. They help deny critical information by controlling the raw data and enhance friendly capabilities by increasing the potential for surprise and effectiveness of friendly military forces and weapons systems.

2.6.1. OPSEC measures consist of a combination of offensive and defensive IO that counter an adversary's ability to "gain" and "exploit" friendly information. These measures must be implemented as part of an overall IO effort to influence the adversary's perceptions and situational awareness.

2.6.2. OPSEC measures fall under three general categories: 1) Preventing the adversary from detecting critical information and indicators; 2) providing alternative deceptive interpretations of critical information and/or indicators; and 3) attacking the adversary's collection system.

2.6.2.1. Preventing adversary detection. A primary OPSEC goal is to mask or control friendly actions to prevent the collection of critical information or indicators. This includes use of protective measures to create closed information systems, such as cryptographic protection and standardized security procedures. Also included in this category of OPSEC is the use of counterintelligence and security forces to thwart access by foreign human intelligence agents.

2.6.2.1. (AFMC) AFMC Product, Logistics, Test Center, and site OPSEC PMs will ensure they or their subordinate unit OPSEC PMs conduct an OPSEC vulnerability assessment in all areas that foreign nationals will reside or visit prior to a foreign national entering the facility. These OPSEC vulnerability assessments are not necessarily formal assessments but walk-through reviews by the OPSEC PM and other organizational personnel to determine what the visitor might see that would identify vulnerabilities. They must be completed in time to correct or change items that need it prior to the arrival of the foreign national(s).

2.6.2.2. Providing alternative interpretations. Sometimes it may not be cost-effective to control actions that reveal critical information or become the source of an OPSEC indicator. In these circumstances, attempts to disrupt or confuse the adversary's ability to properly interpret the information may be required. Use of diversions, camouflage, concealment, and deception are examples of this category.

2.6.2.3. Attacking adversary collection systems. The third type of OPSEC measure is to use IW capabilities to attack an adversary's intelligence collection system and thus eliminate or reduce their ability to obtain critical information. This category includes electronic attack against technical collection platforms and physical destruction of intelligence fusion and analysis centers.

Chapter 3

AIR FORCE OPSEC PROGRAM

3.1. Purpose. T. he purpose of the Air Force OPSEC program is to provide commanders with standardized policy and to facilitate effective OPSEC programs by promoting general understanding and awareness regarding the integration and application of OPSEC. An overall AF OPSEC program manager is identified within the Air Staff to advise on the integration of OPSEC into Service-wide efforts and to develop policy and guidance that provides coordination, training, education, and recognition for unit OPSEC programs.

3.2. Training and Education.. OPSEC training provides Air Force personnel (military and civilian) with a general knowledge of the OPSEC process. The purpose is to ensure Air Force personnel understand the positive benefits of OPSEC and their individual responsibilities; the role of OPSEC as a constituent element of IO; the foreign intelligence threat to friendly operations and the potential effect on mission effectiveness and how the Air Force uses OPSEC measures to minimize the exploitation of critical friendly information.

3.2.1. OPSEC education is a continuing requirement. It must be provided to personnel upon their initial entrance into military service and upon assignment to new organizations. Contractors must ensure employees receive OPSEC training upon initial assignment to a contract with OPSEC requirements (see **2.2.4.**) and civilian personnel must receive OPSEC training upon accession and upon transfer to a new organization.

3.2.1. (AFMC) AFMC Product, Logistics, Test Center, and site OPSEC PMs develop and monitor OPSEC education programs for their activity with the assistance of the AFMC OPSEC PM. Maximize the use of the Interagency OPSEC Support Staff (IOSS) computer based, in residence, and mobile training team classes, website (www.IOSS.gov), posters, and other products to enhance OPSEC awareness/education programs.

3.2.2. Education topics must include the purpose of OPSEC, the role of OPSEC within IO, the OPSEC process, the unit OPSEC program, and awareness of the foreign intelligence threat.

3.2.3. Unit-specific OPSEC training should be provided as part of inprocessing for all new personnel and before individuals receive access to mission critical information. Refresher training should occur at least annually thereafter.

3.2.4. OPSEC Program Manager (PM) Training. OPSEC PM training is required for all individuals designated as OPSEC PMs at wing (or wing-equivalent) level and above, Information Warfare Flight OPSEC POCs, personnel assigned to the Air Force Information Warfare Center (AFIWC) in support of the Air Force OPSEC program, and those who conduct formal OPSEC surveys. The office of primary responsibility (OPR) for OPSEC PM training is AFIWC; HQ USAF/XOIWI will review curriculum for AF OPSEC PM courses each year or whenever changes occur.

3.2.4. (AFMC) AFMC Product, Logistics, Test Center, installation, and site OPSEC PMs must successfully complete the Air Force OPSEC Program Manager's Course. Contact HQ AFMC/SFXP for training allocations. Completion of the IOSS 380 OPSEC course in-residence will satisfy this requirement. Courses are unit funded.

3.2.5. (Added-AFMC) All AFMC military, civilian, and contractor personnel are responsible for understanding the OPSEC concept and the intelligence threat to AFMC operations and resources. Each must apply this understanding to their assigned duties.

3.3. Funding.. HQ USAF/XO will program for and fund the HQ USAF OPSEC program billets and associated activities deemed necessary to orchestrate the Air Force OPSEC program.

3.4. Policy and Evaluation.. HQ USAF/XOIWI will coordinate and evaluate policy for the Air Force OPSEC Program based on Department of Defense and joint policy guidelines, feedback received from Inspectors General (IG) reports, trends identified by AFIWC organizational surveys and feedback from OPSEC PMs.

3.4. (AFMC) Submit requests for interpretation or clarification of policy through OPSEC PM channels to HQ AFMC/SFXP.

3.5. Coordination.. HQ USAF/XOIWI will coordinate OPSEC programs and activities across MAJCOM lines of authority and with organizations outside the Air Force. Direct liaison authority also exists between HQ USAF/XOIWI, AFIWC, HQ AFOSI/XOQ, MAJCOMs, FOAs, and DRUs.

3.6. Reporting.. The AF OPSEC program's reporting requirements include one annual report and two types of time-sensitive reports. MAJCOMs complete a report on the overall OPSEC program once a year that is fed into the annual Defensive Counterinformation assessment IAW AFPD 10-20. Time-sensitive OPSEC Event Reports and OPSEC Advisory Reports are generated by units throughout the year on a case-by-case basis.

3.6. (AFMC) Center and site OPSEC PMs submit annual reports to HQ AFMC/SFXP by 15 November of each calendar year. See AFI 10-1101, Attachment 6, for format.

3.6.1. OPSEC Event Reporting. An OPSEC event consists of inadvertent disclosure of critical information or OPSEC indicators that could jeopardize operations. OPSEC events can be identified as incident to an in-house survey, IO Red Teaming, or discovery by any member of a unit who observes an event during day-to-day operations. In some cases, these events will warrant dissemination beyond the particular unit to enable damage control measures to minimize potential exploitation by adversaries and ensure implementation of Service-wide corrective measures. Commanders retain ultimate authority for determining which events warrant reporting outside their organization. This reporting is not intended to assign blame or initiate punitive action, but rather to highlight potential vulnerabilities, identify trends, and improve Service-wide OPSEC posture. OPSEC PMs are the focal point for ensuring commanders are advised of local OPSEC events and for reporting them as part of the AF's overall defensive counterinformation event reporting procedure being developed IAW AFPD 10-20 and AFI 10-2001 (draft).

3.6.2. OPSEC Advisory Reporting. An OPSEC Advisory Report provides advance notification of a potential threat to OPSEC. Examples include flight paths of foreign aircraft over US territory, locations of foreign naval vessels with collection capabilities, and projected commercial satellite exploitation. Air Intelligence Agency's (AIA's) defensive counter-information fusion center provides OPSEC Advisory Reports as required. OPSEC PMs must review OPSEC Advisory Reports and ensure commanders are informed.

3.7. (Added-AFMC) Program Nickname. The Air Force Materiel Command OPSEC program nickname is CORAL DRAGON, symbolic of the original OPSEC survey, PURPLE DRAGON, conducted during the Vietnam era. Use the purple winged dragon or variations for training purposes and program awareness initiatives.

Chapter 4

UNIT OPSEC PROGRAM

4.1. Purpose and Composition.. Effective unit OPSEC programs support the commander's efforts to accomplish a successful and effective mission. Each program is composed of an OPSEC Program Manager/Point of Contact (the facilitator), OPSEC plans, funding, training, and feedback. Unit OPSEC programs must have the following requisite aspects: Command Involvement, Operational Orientation, Integration, Coordination, and Self-Inspection.

4.1. (AFMC) AFMC organizations at AFMC centers or sites will participate in the center or site OPSEC program. AFMC organizations located on another MAJCOM's installation will participate in the host's OPSEC program. If the host has no OPSEC program, the tenant will participate in the AFMC program.

4.1.1. Command Involvement. Commanders are responsible for ensuring OPSEC guidance is integrated into day-to-day activities. In the spirit of "train as we fight," this fosters seamless transition from peacetime to contingency operations. Commanders may delegate authority for OPSEC program management, but retain responsibility for risk management decisions and the overall implementation of OPSEC measures.

4.1.2. Operational Orientation. The OPSEC program is an operations management program and its goals are information superiority and optimal mission effectiveness. The emphasis is on OPERATIONS and the assurance of effective mission accomplishment. The office of primary responsibility (OPR) should reside in the Plans or Operations element of an organization to ensure effective implementation across organizational and functional lines.

4.1.2. (AFMC) Organizational placement of the OPR at AFMC field activities is at the commander's discretion. However, commanders should consider co-locating the OPR with program protection or force protection personnel to ensure effective implementation across organizational and functional lines.

4.1.3. Integration. OPSEC will be integrated into all organizational plans and activities. Staff elements and supporting organizations must ensure OPSEC procedures are appropriately incorporated—at the earliest possible time—into all operations plans (OPLANs), concept plans (CONPLANs), operations orders (OPORDs), exercise plans, Mission Needs Statements (MNS), Operational Requirements Documents (ORD), program protection plans (PPP), operating procedures and other plans and activities to ensure consistent control of critical information and OPSEC indicators.

4.1.3. (AFMC) OPSEC PMs at all levels must have full knowledge and understanding of the operations and activities of their organizations. The OPSEC PM must have a close working relationship with personnel responsible for plans and operations within the organization. Together they determine the sensitivity of each plan or operation and identify operational vulnerabilities. Vulnerabilities should be eliminated if possible, or reduced by acceptable compensatory measures. When neither elimination nor reduction is possible or practical, conduct a risk assessment to evaluate the consequences of continuing the plan or operation.

4.1.3.1. OPSEC must be an integral part of an overall IO effort. This applies to other DCI functions that also protect friendly information, as well as Offensive Counterinformations (OCI)

functions that influence adversary information. Integration of OPSEC and Public Affairs is particularly important as the need to protect critical information must be balanced against the desire to provide information to the American public.

4.1.3.2. OPSEC is integrated into the Air Operations Center (AOC) through the Information Warfare Flight (IWF). IWF point of contacts (POCs) work within the AOC to ensure planning and execution of air, space, and information operations incorporate OPSEC requirements. IWF OPSEC POCs work with the rest of the IWF to integrate OPSEC with other IO functions. When an AOC is formed, IWF OPSEC POCs become the focal point for integrating the activities of supporting unit OPSEC PM. This ensures the COMAFFOR (Commander Air Force Forces) has a coherent OPSEC effort across all Air Force units.

4.1.3.3. For intertheater air mobility operations, IWF OPSEC POCs are the focal point for planning and integrating OPSEC into intertheater airlift missions on a continuous basis. This is accomplished by working within the Tanker Airlift Control Center at HQ USTRANSCOM.

4.1.4. Coordination. Individuals must protect critical information from all sources and at all levels. Coordination across functional and organizational lines facilitates OPSEC planning and enhances the effectiveness of OPSEC measures. In addition, commanders and/or OPSEC PMs must closely coordinate with intelligence and counterintelligence organizations to identify potential adversaries, intelligence collection capabilities and intentions, and support OPSEC survey efforts.

4.1.4.1. To ensure OPSEC is integrated into IO, OPSEC PMs must work with counterpart personnel working other IO issues for their organization. Although not an IO function, Public Affairs must also be closely integrated into OPSEC efforts by OPSEC PMs.

4.1.4.2. Organizations preparing to deploy, such as an Expeditionary Air Wing, must coordinate OPSEC issues with the gaining command's OPSEC PM.

4.1.5. Self-Inspection. MAJCOM , FOA, and DRU PMs will accomplish annual self-inspections of OPSEC programs and requirements. Other PMs are encouraged to do the same. Self-inspections will be tailored to the functions of the organization.

4.1.5.1. (Added-AFMC) AFMC Product, Logistics, Test Center, and site OPSEC PMs coordinate the OPSEC program within their organization and ensure subordinate units/elements within their oversight have viable OPSEC programs. OPSEC PMs perform staff assistance visits to subordinate elements at least annually, providing advice, assistance, and support. They perform OPSEC assessments on their own initiative (with the concurrence of the commander, director, manager of the surveyed elements), when requested by unit commanders/directors, or as directed by higher headquarters.

4.2. OPSEC Program Managers (PMs).. OPSEC PMs will be assigned IAW AFPD 10-11. Organizations at Wing or Wing-equivalent level and below that do not have OPSEC PMs should assign an OPSEC point-of-contact (POC) to work with PMs at higher headquarters and help ensure critical information is protected within their unit. If OPSEC is assigned as an additional responsibility, it should be combined with other IO activities to provide synergistic mission enhancement.

4.2.1. In the acquisition environment, OPSEC PMs must work directly with program directors to ensure OPSEC principles are integrated and applied throughout the life cycle of all programs. Contractor support must also be taken into consideration as part of OPSEC programs.

4.2.2. OPSEC PMs are responsible for advising commanders (and/or program directors) on OPSEC related matters, facilitating OPSEC implementation, and managing the organization's OPSEC program.

4.2.3. OPSEC PMs must be familiar with the unit goals, objectives, strategies, activities, and personnel who participate in those activities.

4.2.4. (Added-AFMC) All AFMC Product, Logistics, and Test Centers, and AFMC sites will designate a primary and alternate OPSEC PM in writing. Send letters of appointment to HQ AFMC/SF; update appointment letters as changes occur. Appointment letters will include:

- Name
- Rank or Grade
- Security Clearance
- DSN/Commercial Telephone Number
- STU III or STE Number
- FAX Number/Secure FAX Number
- E-Mail address
- Mailing Address
- Office Symbol and Duty Title

4.2.4.1. (Added-AFMC) All subordinate two-letter organizations or units will designate a primary and alternate OPSEC PM in writing. Send the letter of appointment to the center or site OPSEC PM. Update appointment letters as changes occur. Include the same information as required in paragraph 4.2.4 above.

4.3. OPSEC Planning.. All Air Force organizations conducting or supporting operational missions must integrate OPSEC into their planning and develop OPSEC plans to ensure critical information and indicators are protected.

4.3. (AFMC) OPSEC PMs at all levels must review the OPSEC annex in operations, wartime, contingency, and exercise plans that impact their organization at least annually. The OPSEC annex for each plan must include a list of CI applicable to the operation.

4.3.1. OPSEC requires deliberate and continuous planning. Deliberate planning ensures OPSEC is implemented in a proactive manner and integrated into all operations and support activities. Continuous planning ensures flexibility and improvements in the fact of changing missions and threats.

4.3.2. OPSEC Plans. Each MAJCOM will have a written OPSEC plan (see **Attachment 7** for format). An OPSEC plan can be a separate plan, an annex to a larger plan, or the integration of OPSEC into an overall mission plan. OPSEC plan considerations include, but are not limited to:

4.3.2. (AFMC) AFMC Centers and sites will have a written OPSEC Plan. An OPSEC plan can be a separate plan, an annex to a larger plan, or the integration of OPSEC into an overall mission or program protection plan. OPSEC Plans will be reviewed/updated by the OPSEC PM annually for OPSEC currency. The OPSEC Plan will include the following:

- References
- General Mission/Program Description
- Security Responsibilities
- Critical Information list
- Indicators
- Threat
- Vulnerabilities
- Countermeasures
- Public Affairs
- Training
- Supporting Units/Associated Programs

4.3.2.1. Command Guidance. An essential part of the OPSEC plan is clear direction for participating organizations to protect critical information and the indicators of such information to prevent exploitation. Command guidance should include direction to continuously monitor and review friendly activities to identify changing parameters as operations mature.

4.3.2.2. Critical Information. OPSEC plans must identify critical information and OPSEC vulnerabilities applicable to the mission. OPSEC planners must consider adversarial objectives, the knowledge they need to effectively plan against friendly forces, and their capability to gain such information.

4.3.2.3. Intelligence Threat Information. Air Force intelligence and counterintelligence organizations will provide intelligence threat information which should include the following:

4.3.2.3.1. Adversary intelligence collection capabilities, presence, and intentions. These factors must be continually assessed throughout the duration of each operation.

4.3.2.3.2. Adversary critical information requirements. When adversary information requirements pertinent to the existing or planned situation are known, they will be listed.

4.3.2.3.3. Probable adversary knowledge. In assessing OPSEC vulnerabilities, OPSEC planners should consider knowledge an adversary may already possess (from general knowledge, open sources, or from what is inevitably revealed when a plan is executed to determine OPSEC vulnerabilities.

4.3.2.4. OPSEC Indicators. OPSEC plans should address indicators of critical information, that are not currently protected.

4.3.2.5. OPSEC Measures. Once indicators are identified, OPSEC measures should be developed and applied to minimize, alter, or eliminate such indicators.

4.3.2.6. Planning Coordination. OPLANs must be appropriately coordinated with supporting organizations to ensure critical information is consistently protected. Since exploitable

information resides in numerous sources within most Air Force organizations and activities, OPSEC plans must be developed, coordinated, and implemented by all functional areas.

4.3.2.7. Subordinate and Supporting Organizations. When appropriate, subordinate and supporting organizations should develop supporting plans for their specific activities. MAJCOM, NAF, product/logistic/test centers, and wing plans will identify supporting organizations that are required to have a written OPSEC plan.

4.4. Unit OPSEC Training.. The purpose of OPSEC training is to ensure personnel are familiar with potential threats related to the unit, critical information for the mission it supports, job specific OPSEC indicators, and the OPSEC measures they will execute. Briefings to new personnel should include duty related critical information and OPSEC indicators; foreign intelligence threat to mission supported and conducted and individual responsibilities.

4.4. (AFMC) The target group for this training is all military, civilian, and resident contractor personnel.

4.5. Funding.. All MAJCOMs, laboratories, product and logistic centers, and test ranges should program for and fund billets for their unit OPSEC PMs. HQ USAF/XO and HQ AIA will ensure AFIWC is provided funds for training aids and materials for use by OPSEC program managers throughout the Air Force.

4.5. (AFMC) Units will provide adequate funding for OPSEC program manager training and OPSEC assessment/survey costs. AFMC Center and site PMs will submit annual OPSEC course projections to HQ AFMC/SFXP.

4.6. Evaluations.. There are several methods used to evaluate unit OPSEC programs and the effectiveness of unit OPSEC measures; in-house OPSEC surveys; OPSEC appraisals; IO Red Teaming (OPSEC multi-disciplinary vulnerability assessments or (OMDVA), telecommunications monitoring, etc.) and Inspector General evaluations.

4.6.1. OPSEC Surveys. Commanders will conduct a comprehensive in-house survey with available resources, on at least an annual basis. Part of an overall IO vulnerability assessment, these surveys consist of an internal assessment conducted by the OPSEC program manager with the support of functional area specialists from within the organization or from the local host unit. The use of this type of survey is encouraged when scheduling or operational tempo does not provide the opportunity for an OMDVA or other IO Red Teaming effort.

4.6.1. (AFMC) Document survey actions in writing and maintain copies with OPSEC records. Organizational/unit OPSEC PMs that require assistance in conducting OPSEC surveys should contact the center or site OPSEC PM.

4.6.1.1. (Added-AFMC) AFMC Center and site OPSEC PMs conduct OPSEC surveys of selected programs and operations. Give particular attention to support of program planning for acquisition programs. OPSEC is a commander's program, hence; AFMC Centers, and sites will request OPSEC Multi-discipline Vulnerability Assessments (OMDVA) through HQ AFMC/ SFXP who will coordinate with AFIWC for the assessment. OMDVAs should be requested at least every five years. HQ AFMC/SFXP will conduct SAVs at least once every three years.

4.6.2. OPSEC Appraisals. While an OPSEC survey evaluates the OPSEC posture throughout an entire organization, an OPSEC appraisal is a timely analysis conducted in support of a specific operation, activity, or exercise. The appraisal is distinguished from the OPSEC survey by the scope and timeliness of the analysis. The appraisal may be as limited as a desktop analysis in response to an operational planner's query, or as extensive as the formation of a multi-disciplinary analytical team to support a particular contingency, exercise, or field operational test and evaluation event.

4.6.3. IO Red Teaming. The most realistic test for an OPSEC program involves use of outside expertise to simulate an IO threat and evaluate the organization's defensive response. IO Red Teaming specifically geared towards OPSEC includes OMDVA and telecommunications monitoring. IO Red Teaming is only done at the request of the unit commander.

4.6.3.1. OMDVA. The AFIWC is the only Air Force agency authorized to conduct OPSEC assessments across organizational boundaries. AFIWC conducts OMDVAs as part of IO Red Teaming. AFIWC personnel, along with augmentation from other organizations, contribute expertise and manpower for these in-depth assessments. HQ USAF, MAJCOMs, and local units (through MAJCOM channels) may request OPSEC assessments from AFIWC. Note that the resources and time required to perform an in-depth OPSEC assessment of this caliber severely limits the potential number possible during any given year.

4.6.3.2. Telecommunications Monitoring. Telecommunications monitoring involves the monitoring and analysis of unsecure voice, fax, data (networks and wireless devices), and other electronic transmissions to evaluate an organization's OPSEC posture. Telecommunications monitoring is accomplished only within certain legal parameters and may only be performed by authorized agencies as outlined in AFI 33-219, *Telecommunications Monitoring and Assessment Program* (TMAP). Telecommunications monitoring is conducted either upon request of an appropriate authority (wing/CC), during OMDVAs, or as an element of the AFIWC IO Red Team.

4.6.4. Inspector General Evaluations. OPSEC program will be evaluated during operational readiness inspections. Additional guidance is provided in AFI 90-201, *Inspector General Activities*. MAJCOM/FOA/DRU's PM will coordinate with their respective IG team to ensure OPSEC evaluation criteria are current and IAW unique guidance from the MAJCOM/FOA/DRU commander.

ROBERT H. FOGLESONG Lt General, . USAF
DCS/Air and Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, October 23, 2000

DoD Directive 5205.2, *DoD Operations Security (OPSEC) Program*, November 29, 1999

CJCSI 3210.01A, *Joint Information Warfare Policy*, January 2, 1996

CJCSI 3213.01, *Joint Operations Security*, May 28, 1993

AFPD 10-11, *Operations Security*

AFPD 10-20, *Air Force Defensive Counterinformation Operations*

AFPD 31-1, *Physical Security*

AFPD 31-4, *Information Security*

AFPD 31-7, *Acquisition Security*

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*

AFI 33-129, *Transmission of Information via the Internet*

AFPD 33-2, *Information Protection*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFI 90-201, *Inspector General Activities*

Terms

Capability—The ability to execute a specified course of action. (A capability may or may not be accompanied by an intention) (Joint Pub 1-02). NOTE: When considering vulnerabilities, a capability requires the physical and mental attributes and sufficient time required for performance.

Counterintelligence—Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (ref. Joint Pub 1-02).

Defensive Counterinformation—Activities which are conducted to protect and defend friendly information and information systems. Also called DCI. (AFDD 1-2)

Exploitation. a.) Taking full advantage of success in battle and following up initial gains. b.) Taking full advantage of any information that has come to hand for tactical or strategic purposes. c.) An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth (Joint Pub 1-02).

Foreign Intelligence—Information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities.

Information Function—Any activity involving the acquisition, transmission, storage or transformation of information. (Cornerstones of Information Warfare)

Information Operations—Actions taken to affect adversary information and information systems while defending one's own information and information systems. See also defensive information operations; information, information system; offensive information operations; operation (Joint Pub 1-02)

Information Warfare—Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries. Also called IW. See also crisis; information operations; operation.

Multi-discipline Counterintelligence Threat Assessment (MDCITA)—All–source (HUMINT, SIGINT, IMINT, and OSINT) analysis of threats to a specific activity, location, operation, project, weapons or other system, deployment, or exercise.

Offensive Counterinformation—Offensive IW activities which are conducted to control the information environment by denying, degrading, disrupting, destroying, and deceiving the adversary's information and information systems. Also called OCI.

OPSEC Advisory—An OPSEC advisory is advance notice of a potential threat to OPSEC. Examples include flight paths of foreign aircraft over-flying US territory, locations of foreign naval vessels with collection capabilities, and projected commercial satellite exploitation.

OPSEC Event.—An OPSEC event consists of inadvertent disclosure of critical information or OPSEC indicator that could jeopardize operations. OPSEC events can be identified as part of an in-house survey, IO Red Team or by any individual that observes the activity. These events are highlighted to enable damage control measures that can avoid potential exploitation by adversaries and ensure future corrective measures are implemented.

OPSEC Vulnerability.—A condition in which friendly actions provide OPSEC indicators that may be obtained and accurately evaluated by an adversary in time to provide a basis for effective decision making. (Joint Pub 1-02)

Attachment 2

RESPONSIBILITIES AND AUTHORITIES

A2.1. Command Responsibilities. Although the OPSEC program helps commanders make and implement decisions, the decisions themselves are the commanders' responsibility. Commanders must understand the risk to the mission and then determine whether OPSEC measures are required. Commanders must make the difficult decisions that involve risks to mission effectiveness.

A2.1.1. Commanders at every level will:

A2.1.1.1. Integrate the OPSEC concept into their mission plans and activities.

A2.1.1.2. Ensure assigned personnel are familiar with OPSEC and its application to organizational effectiveness.

A2.1.1.3. Ensure OPSEC reviews are conducted on unit/organizational web pages.

A2.1.1.4. Ensure OPSEC measures are appropriately developed and executed to reinforce the combat effectiveness of units and weapons systems.

A2.1.1.5. Approve a critical information list for their organization.

A2.1.1.6. Centrally manage OPSEC guidance concerning critical information to ensure consistency throughout each organization and across organizational lines.

A2.1.1.7. Ensure OPSEC events are reported IAW AFPD 10-20 as appropriate.

A2.1.1.8. Provide management, annual review, and evaluation of their OPSEC programs.

A2.1.1.9. Submit an annual OPSEC report to higher headquarters, IAW format provided in **Attachment 6**.

A2.2. Headquarters, United States Air Force (HQ/USAF) Responsibilities. The Deputy Chief of Staff for Air & Space Operations (HQ USAF/XO) is the office of primary responsibility for the Air Force OPSEC program. HQ USAF/XO, through the Defensive Information Warfare Branch (HQ USAF/XOIWI), will:

A2.2.1. Develop OPSEC doctrine, policies, plans, and procedures consistent with joint and DoD OPSEC guidance.

A2.2.2. Designate an overall Air Force OPSEC Program Manager.

A2.2.3. Provide to J-3, Joint Staff, Attn: J-33/STOD/TSB, copies of all current service OPSEC program directives and/or policy implementation documents.

A2.2.4. Support the national and DoD OPSEC programs as necessary.

A2.2.5. Provide management, annual review, and evaluation of the Air Force OPSEC Program.

A2.2.6. Recommend changes to policy, procedures and practices of the DoD OPSEC Program to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD/C3I).

A2.2.7. Utilize OPSEC training advice and services provided by the National Security Agency (NSA) and the Interagency OPSEC Support Staff (IOSS) when appropriate.

A2.3. HQ AFOSI will, upon request from the commander concerned, provide Air Force units with current mission specific counterintelligence and MDCI threat assessment information.

A2.4. Air Force Major Command (MAJCOM), Field Operating Agency (FOA), and Direct Reporting Unit (DRU). MAJCOMs, FOAs, and DRUs will develop effective OPSEC programs that meet the specific needs of their assigned mission and accomplish the following:

A2.4.1. Provide coordination across organizational boundaries as necessary (both vertically and horizontally) to facilitate consistent application of OPSEC throughout the command.

A2.4.2. Ensure critical information is identified for each operation, activity, and exercise whether it be planned, conducted, or supported.

A2.4.3. Provide guidance to subordinate units for controlling critical information and indicators.

A2.4.4. Ensure subordinate units plan, exercise, and implement OPSEC measures as appropriate.

A2.4.5. Develop OPSEC requirements for new weapon and/or defense systems in the acquisition cycle, list such requirements in Mission Needs Statements, and participate in milestone reviews to ensure such requirements are satisfied.

A2.4.6. Develop and cultivate the relationship necessary to ensure intelligence and counterintelligence support requirements for OPSEC programs.

A2.4.7. Ensure OPSEC considerations are included in annual unclassified web pages reviews and in the approval process for posting new data to the web.

A2.4.8. Ensure job oriented and mission specific OPSEC awareness training is provided to all personnel on a recurring basis as often as necessary, but not less than at one-year intervals.

A2.4.9. Ensure OPSEC training of OPSEC PMs at Wing (or Wing-equivalent) level and above upon appointment and on a recurring basis.

A2.4.10. Designate a Program Manager (PM) and an office of primary responsibility IAW AFPD 10-11. The decision to assign a full-time OPSEC PM at FOAs and DRUs rests with the commander based upon the specific needs of the assigned mission.

A2.4.10. (AFMC) The OPSEC PM for AFMC resides in HQ AFMC/SF per authority of HQ USAF/XOXT, “Letter of Deviation,” 9 February 1995.

A2.4.11. Complete annual self-inspections to assess their programs.

A2.4.12. Report OPSEC events to HQ AIA’s defensive counterinformation fusion center in a timely manner IAW AFPD 10-20.

A2.5. Air Intelligence Agency (AIA) will:

A2.5.1. Centrally manage funds for the AF-wide OPSEC program.

A2.5.2. Incorporate OPSEC event reporting into a defensive counterinformation fused Analysis.

A2.5.3. Provide OPSEC advisory reporting to the AF through the Air Force Information Warfare Center.

A2.5.4. Consolidate annual OPSEC reporting into the AF’s DCI annual assessment.

A2.5.5. Ensure IW Flights have OPSEC expertise required to support integration of OPSEC into campaign planning and execution.

A2.5.6. Ensure OPSEC is integrated into IW Tactics, Techniques, and Procedures (TTP).

A2.5.7. Conduct annual OPSEC training for personnel assigned to HQ AIA.

A2.6. Air Force Information Warfare Center. AFIWC will provide administrative support, technical services, and assistance for OPSEC program development, planning, and execution. Direct communication is authorized between AFIWC and the MAJCOM, FOA, and DRU OPSEC program managers. Informal communication is authorized between AFIWC and other Services and DoD agency counterparts for the exchange of information on OPSEC program matters. AFWIC is responsible for providing expertise and manpower for OPSEC assessments and will develop and maintain:

A2.6.1. The capability to accomplish multi-disciplined OPSEC surveys as part of an integrated IO red team.

A2.6.2. OPSEC training aids and materials to support an active marketing and training program to be presented by OPSEC PMs in the field.

A2.6.3. A training course for OPSEC program managers and other personnel who perform OPSEC surveys.

A2.7. The National Air Intelligence Center (NAIC) will provide foreign intelligence threat information to all Air Force units and supporting organizations. Threat information will identify current and potential adversaries and include foreign intelligence capabilities, intentions, resources, doctrine and state-of-the-art intelligence collection methods. The report will be updated on at least an annual basis.

A2.8. Air Force Information Warfare Battlelab will be clearinghouse for new ideas to improve OPSEC.

A2.9. Air Force Office of Special Investigations (AFOSI). AFOSI is the sole agency within the Air Force chartered to perform the counterintelligence mission. AFOSI will support OPSEC PMs and commanders with OPSEC survey support, MDCI Threat Assessments, planning and training assistance, and a complete range of studies, reports, and analytical products. AFOSI detachment commanders will assist their local commanders with access, as necessary, to threat information from sources outside the Air Force. AFOSI will support NAIC in developing an annual all-source intelligence report of the OPSEC threat to the Air Force.

A2.10. Air Education and Training Command (AETC) Responsbilities. Air Education and Training Command (AETC) will provide for a basic, but thorough, introduction of OPSEC to all new (military) Air Force members. The block of training must include:

A2.10.1. The purpose and value of the OPSEC concept.

A2.10.2. An overview of the process.

A2.10.3. An introduction to the application of OPSEC measures.

A2.11. OPSEC will be presented as “this is the way we do our day-to-day business in the United States Air Force.” AETC will also provide general OPSEC education, as appropriate, in all professional level

courses. Professional level material should include the purpose and use of the OPSEC concept, the process, complementing and conflicting concepts, OPSEC planning, and command responsibilities.

Attachment 3

SOURCES OF OPSEC INDICATORS

Note: This list is NOT all-inclusive. It is provided as a stimulus only.

A3.1. Operational Indicators:

A3.1.1. Stereotyped activities such as schedules, test preparation, range closure.

A3.1.2. Visits of VIPs associated with a particular activity or technology.

A3.1.3. Abrupt changes or cancellations of schedules.

A3.1.4. Specialized equipment.

A3.1.5. Specialized training.

A3.1.6. Increased telephone calls, conferences, and longer working hours (including weekends).

A3.1.7. Rehearsals of operations.

A3.1.8. Unusual or increased trips and conferences by senior officials.

A3.1.9. Implementation of Threat Conditions (THREATCONs) and Information Operations Conditions (INFOCONs).

A3.2. Communications Indicators:

A3.2.1. Specialized and unique communications equipment.

A3.2.2. Power sources.

A3.2.3. Increases and decreases in communications traffic.

A3.2.4. Call signs.

A3.2.5. Transmitter locations.

A3.2.6. Increase in network traffic/encrypted network traffic.

A3.2.7. Increase in remote dial-ups from home.

A3.3. Administrative Indicators:

A3.3.1. Military orders.

A3.3.2. Distinctive emblem, logos, and other markings on personnel, equipment, and supplies.

A3.3.3. Transportation arrangements.

A3.3.4. Schedules, orders, flight plans, and duty rosters.

A3.3.5. Leave cancellations.

A3.4. Logistics and Maintenance Support Indicators.

A3.4.1. Unique sized and shaped boxes, tanks, and other containers.

A3.4.2. Pre-positioned equipment.

A3.4.3. Technical representatives.

A3.4.4. Maintenance activity.

A3.4.5. Unique or special commercial services.

A3.4.6. Deviations of normal procedures.

A3.4.7. Physical security arrangements.

Attachment 4

UNIT OPSEC PM/POC DUTIES

1. Facilitating the implementation of OPSEC throughout their organization

2. Integrating OPSEC into organizational plans and activities

3. Advising commanders and other decision makers on OPSEC matters

4. Coordinating on (and facilitating the development of) OPSEC plans and measures for operations, activities, and exercises

5. Ensuring OPSEC reviews are conducted on all organizational/unit web pages.

6. Integrating OPSEC requirements into IO/IW and force protection strategies

7. Developing and maintaining the organization's OPSEC program

8. Ensuring all personnel receive appropriate OPSEC training

9. Conducting annual OPSEC self-inspection and OPSEC appraisals (as directed)

10. Maintaining effective rapport with intelligence and counterintelligence agencies and providing OPSEC program requirements for intelligence and counterintelligence support

11. Coordinating OPSEC requirements with public affairs officers

12. Coordinating with activities which complement OPSEC

13. Ensuring critical information is identified and controlled

14. Assisting in determining operational requirements for security and guidelines for the release of information

15. Determining guidelines for controlling critical information and sensitive activities

16. Coordinating and facilitating OPSEC surveys

17. Ensuring OPSEC considerations are included in posting of new data to the NIPRnet/internet and reviewing organizational web pages on an annual basis.

18. Drafting annual OPSEC report for submission by the commander to higher headquarters

19. Forwarding recommendations for change or program modification to HQ USAF/XOIWD through appropriate channels

20. Serve as focal point for OPSEC event reporting IAW AFPD 10-20 & AFI 10-2001 (when published).

21. (Added-AFMC) In addition to PM duties listed, AFMC Product, Logistics, Test Center, and site PM duties include, but are not limited to:

- Identifying OPSEC PMs at unit levels as required.
- Establishing an OPSEC working group as a staff forum for addressing command and local OPSEC policies, programs, and objectives. The working group must convene at least semi-annually. Send copies of working group minutes to HQ AFMC/SFXP.
- Coordinating with local protective security functions and AFOSI to ensure adequate funding for security countermeasures as determined necessary by OPSEC assessments.
- Ensuring OPSEC reviews are conducted on all organizational/unit web pages annually IAW AFI 10-1101, attachment 4, paragraph 5.
- Ensuring vulnerability assessments are conducted on all areas where foreign nationals are housed or visit prior to their arrival within the organization.
- Establishing and maintaining a comprehensive continuity file.
- Supplementing this publication as necessary. Notifying HQ AFMC/SFXP when supplement is published.

22. (Added-AFMC) HQ AFMC/SF is the OPR for Military Deception (MD), formerly known as Tactical Deception (TD). Coordinate MD operations with this office. The OPSEC OPR for AFMC centers, site, and subordinate organizations will be the MD focal point.

Attachment 5

SAMPLE OPSEC SELF-INSPECTION CHECKLIST

1. Has a unit or staff agency OPSEC program manager (PM) or point of contact (POC) been appointed in writing?

a. Is the appointee from the plans or operations element?

b. Has the identity of the OPSEC PM/POC been forwarded to higher headquarters OPSEC office of primary responsibility (OPR)?

c. Are visual aids identifying the OPSEC PM/POCs prominently displayed throughout the unit or staff agency?

d. Are the unit or staff agency OPSEC PM/POCs aware of their responsibilities (see Attachment 4)?

e. Does the OPSEC PM/POC attend and address OPSEC matters at unit security awareness and education meetings?

f. Has the unit OPSEC PM/POC attended or requested to attend the USAF OPSEC Program Managers' Course through their MAJCOM, FOA, or DRU OPSEC OPR?

2. Has the OPSEC PM/POC established a continuity folder?

a. Are current editions of all instruction, pamphlets, and directives (JCS Pub 3-54, AFPD 10-11, AFI 10 1101, MAJCOM Sups) available?

b. Does the unit have local directives that define unit OPSEC program requirements, responsibilities, and procedures?

c. Does the continuity folder include files of past OMDVAs, surveys, and appraisals?

d. Does the OPSEC PM/POC keep files of past OPSEC event and advisory reports?

3. Does the commander actively advocate, support, and implement OPSEC options in support of the operational mission and exercises?

a. Has the commander signed an OPSEC policy letter supporting the program?

b. Is the unit Critical Information List (CIL) reviewed and approved by the Commander?

c. Is OPSEC addressed at Commander's Call?

4. Does the unit OPSEC program promote active participation and involvement of all personnel?

a. Are OPSEC posters prominently displayed throughout the unit?

b. Is OPSEC education material reaching all unit personnel?

c. Is the unit CIL tailored to each functional activity?

(1) Is the CIL specific, realistic, and current?

(2) Are unit or functional area CILs easily accessible to unit personnel?

(3) Are unit personnel familiar with their portion of the CIL?

(4) Is the CIL unclassified to allow for maximum dissemination?

5. Does the unit OPSEC program include provisions for reviewing plans, operations orders (OPORD), and exercise scenarios?

a. Is current potential adversary threat data maintained and considered in plans and exercises?

b. Do unit plans or OPORDS, contain, as a minimum, the purpose and current definition of OPSEC, the foreign intelligence Threat, and specific CILs?

6. Are the interrelationships of OPSEC, communications security (COMSEC), computer security (COMPUSEC), physical security, and information security program clearly understood by the OPSEC POC?

7. Has the unit OPSEC PM/POC coordinated with other unit security managers (e.g., COMSEC, Information Security, and COMPUSEC), to incorporate OPSEC concepts and lessons learned into security training sessions?

8. Has the unit OPSEC PM/POC established and maintained liaison with the base or higher headquarters OPSEC PM?

9. Is OPSEC training related to the unit mission, tailored to individual duties and responsibilities, and presented to newly assigned personnel upon initial assignment and at least annually thereafter?

10. Does unit OPSEC training contain the following:

a. The OPSEC methodology?

b. Duty related critical information and OPSEC indicators?

c. Foreign intelligence threat to the unit mission?

d. Individual responsibilities?

e. OPSEC and its relationship to IO?

11. Has the OPSEC PM/POC submitted an annual OPSEC Report?

12. Has an OPSEC survey or appraisal been conducted?

a. If yes:

(1) Are the results easily accessible?

(2) Have results been addressed through unit awareness programs?

(3) Has unit mission or CIL changed significantly to warrant a new survey?

b. If no, has one been scheduled or requested?

13. Have actions been taken to act on recommendations or to correct weaknesses and deficiencies noted in the OPSEC survey?

14. Are all OPSEC recurring publications (e.g., the OPSEC update, COMSEC quarterly analysis, etc.) reviewed for OPSEC lessons learned?

15. Do official and unofficial feedback publications such as unit newsletters contain sensitive or classified information? If so, are they protected?

16. Do indexes for directives and operating instructions reveal sensitive operations or functions?

17. Do unclassified computer products disclose sensitive mission activity?

18. Are ADPE (Automated Data Processing Equipment) products protected and destroyed as classified waste? i.e. typewriter ribbons, disks, etc)

19. Is the OPSEC PM/POC on distribution for telecommunications monitoring or AFOSI HUMINT Vulnerability Assessments reports involving their unit?

20. Is OPSEC included in the process for posting and reviewing information on organizational web-pages?

Attachment 6

ANNUAL OPSEC REPORT FORMAT

Training. Provide status of OPSEC training over the last year. Include number of personnel trained and total in unit.

Self-Inspection. Provide date of last self-inspection (see **Attachment 5** for checklist). Include brief summary of any results OPSEC PM believes should be highlighted.

In-house Survey. Provide date of last in-house survey. Include results that OPSEC PM believes should be highlighted.

OMDVA/TMAP/IO Red Teaming. Provide date of last OMDVA/TMAP/IO Red Team activity. Include results that OPSEC PM believes should be highlighted.

MDCI TA. Provide date of last MDCI report provided by AFOSI.

OPSEC Plans. Provide listing of the unit's OPSEC plans and date of last review (see **Attachment 7** for plan format).

Lessons Learned/Recommendations. Provide any additional information regarding specific OPSEC lessons learned or recommendations for improving OPSEC implementation.

POC. Provide list of OPSEC POCs.

Note: Units will submit their reports to headquarters, such that NAFs will correlate data from wings, and MAJCOM reports will correlate data from subordinate NAFs.

Example: Self-Inspection.

HQ PACAF. Conducted 15 Oct 00.

HQ 5AF. Conducted 1 Sep 00.

432 FW. Conducted 12 Jun 00.

18 FW. Conducted 5 Jun 00.

HQ 7AF. Conducted 8 Aug 00.

Etc.

MAJCOMS should include their annual OPSEC report as an appendix to the annual Defensive Counterinformation assessment report provided to HQ AIA, per AFPD 10-20 and AFI 10-2001 (when published).

Attachment 7

OPSEC PLAN FORMAT

1. References

2. General Mission/Program Description

3. Security Responsibilities

4. Critical Information List (CIL) (see **Chapter 2**)

5. Indicators (see **Chapter 2** and **Attachment 3**)

6. Threat (see **Chapter 2**)

7. Vulnerabilities (see **Chapter 2**)

8. Countermeasures and Risk Assessment

9. Public Affairs

10. Training (see **Chapter 3**)

11. Supporting Units/Associated Programs